Augmented Borders: Big Data and the Ethics of Immigration Control

Abstract

Investment in the technologies of borders and their securitisation continues to be a focal point for many governments across the globe. This paper is concerned with a particular example of such technologies, namely 'Big Data' analytics. In the last two years, the technology of big data has gained a remarkable popularity within a variety of sectors, ranging from business and government to scientific and research fields. While big data techniques are often extoled as the next frontier for innovation and productivity, they are also raising many ethical issues. The aim of this article is to consider some of these issues in light of the application of big data in the domain of border security and immigration management. I draw on the example of the new big data solution recently developed by IBM for the Australian Customs and Border Protection Service. The system, which relies on data collected from Passenger Name Records, aims to facilitate and automate mechanisms of profiling in order enable the identification of 'high risk' travellers. I argue that the use of such big data techniques risks *augmenting* the function and intensity of borders. The main concerns I address here revolve around three key elements, namely, the problem of categorisation, the projective and predictive nature of big data techniques and their approach to the future, and the implications of big data on understandings and practices of identity. By exploring these issues, the paper aims to contribute to the debates on the impact of ICT-based surveillance in border management.

Keywords: Big Data, borders, categorisation, ethics, identity, immigration, projection

Augmented Borders: Big Data and the Ethics of Immigration Control

Borders and their securitisation continue to be a major concern for governments across the world. Advanced information systems and technologies are increasingly being looked up to as a solution for managing the flow of people and things. Recently, there has been a growing interest in "Big Data" analytics and its potential to enhance the means by which vast data can be effectively analysed and transformed into more fine grained knowledge to enable faster and more advanced decision making processes vis-à-vis access, or denial of it, across international borders. In Australia, for instance, the Department of Immigration and Citizenship (DIAC) has developed the Border Risk Identification System (BRIS) which relies on big data tools to construct patterns and correlations for improving border management and targeting so-called 'risky travellers' (*Big Data Strategy*, 2013). While in Europe, programmes such as European border surveillance system (EUROSUR) and Frontex are examples of ICT-mediated surveillance whereby big data techniques are increasingly utilised for predicting, monitoring and controlling movements across EU borders. And it is just a matter of time before other countries start adopting big data for the governance of immigration. Despite this increasing interest in big data within immigration policy, border management, and beyond, there is a marked absence of studies that directly deal with the wider impacts of big data on immigration politics and governance, as the majority of available literature on big data tends to mainly focus on their popularity and potential for value-creation. As a response and by referring to the example of Australia's recently developed Border Risk Identification System, this paper looks at the relation of big data to borders and addresses some of the ethical implications of such techniques in the management of immigration and movement. I begin with an examination of the concept of big data itself followed by a reflection on borders and their redefinition by way of opening up a discussion on the implications of big data vis-à-vis immigration governance. Three interrelated concerns are being examined throughout this paper. First, I discuss the issue of 'categorisation' and its far-reaching impacts that touch the very question of the 'human' itself. The second issue relates to 'projection' and the predictive nature of big data. I argue that the analytic techniques of big data encourage a preemptive and parochial attitude towards the future, and enable the systematic profiling of people and the forming of various categorical assumptions about their character and risk potential. The third issue concerns the

question of 'identity' and its conceptualisation in big data. Here, I stress the importance of embodiment in understanding what is at stake in the management and control of identity through big data for the purpose of immigration and border management. In light of these concerns, the paper advocates an *embodied* ethical approach to borders, one that can recognise the corporeal conditions and material consequences of big data use, and leverage against the security-driven and fear-based visions currently perpetuated by data industries and governmental institutions alike.

The rise of Big Data

Recently, the buzzword of big data has invaded many spheres of production, knowledge and expertise. From marketing and advertising to healthcare and bioinformatics, various fields are currently exploring the possible benefits and challenges pertaining to the collection and usage of large data sets for different purposes and contexts. Generally, big data are often defined as 'datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze' (McKinsey Global Institute, 2011), requiring as such more enhanced technologies and advanced analytic capabilities. The purpose of big data analytics is very much about prediction and decision-making, focusing on 'why events are happening, what will happen next, and how to optimize the enterprise's future actions' (Parnell in Field Technologies Online, 2013). Big data[1] are aggregated from a variety of sources including social media, web search histories, online transactions records, mobile technologies and sensors that gather information about location, and any other source where digital traces are left behind knowingly or unknowingly. Some of these data are actively volunteered by users and consumers on networking sites, for instance, while others are collected through various means and technologies embedded within the routine activities of everyday life. Given the rise of social networking and mobile technologies and the ever-increasing digitisation of work, leisure and daily actions and habits, the quantity of data being generated today has reached an unprecedented scale. According to IBM calculations, prior to 2003 five exabytes (five billion gigabytes) of data have been generated. In 2011, that amount was produced every two days and in 2013 that much was generated every 10 minutes (Rieland, 2012; Harpertill, 2013; IBM, 2013).

Although emphasis is often placed on the 'size' aspect, it is worth bearing in mind that big data are by no means merely about large data. In fact, big data are above all networked relational data (Manovich, 2011; Boyd and Crawford, 2011). The size is certainly an important characteristic but, on its own, does not lend big data its major importance in the science of data or the computational culture. It is the power of connecting, creating/unlocking patterns and visualising relations that makes big data such a seductive field of investment and enquiry for many sectors and organisations. As Boyd and Crawford (2011) explain, 'Big data tempts some researchers to believe that they can see everything at a 30,000-foot view. It is the kind of data that encourages the practice of apophenia: seeing patterns where none actually exist, simply because massive quantities of data can offer connections that radiate in all directions'.

To be sure, this is not the first time we are witnessing an avalanche of data that promises different ways of 'seeing' the world and uncovering its manifold connections. From Domesday Book to modern statistics, from photography to advances in molecular biology, history is littered with examples whereby the availability of new data and their accumulation have facilitated new ways of perceiving the world and understanding the social, oftentimes with material real-world consequences. Ian Hacking (1990) considers the exponential growth of statistical data and their use during the 19th century as an 'avalanche of numbers' that had a profound impact on the definition and demarcation between what is normal and what is deviant, and on the organisation of human behaviour in various spaces and practices ranging from factories and schools to the military and hospitals. Numbers became not only a means of measuring but also a highly politicised tool of managing and disciplining individuals and populations. Statistics, as such, has influenced much of the social and scientific ways of thinking and acting in the nineteenth and twentieth century. As Latour (2000) reminds us '[c]hange the instruments, and you will change the entire social theory that goes with them'.

Today, a similar thing might be occurring through big data: new ontologies and new metaphors about the world and social processes are emerging and in ways that are undoubtedly reconfiguring the relation between individuals and groups, between the local and the global, between the digital and the physical and so on. What is at issue is not merely data or their volume, but also the kind of discourses and rationales, the

styles of thought and strategies that surround emergent modes of organising and categorising the world and the living. In all these, assumptions, biases and power structures abound.

Questions are thus being raised about the possible impacts of big data. Will large-scale data analytics enhance the efficiency and effectiveness of informational processes thereby yielding economic and social benefits? Or will it reinforce existing inequalities and create further threats to familiar issues like privacy and data protection? There is, in a sense, nothing new about such questions. Each time a new technique or technology comes about, there emerge with it a whole host of fears and promises that are often technologically deterministic. Examples from media technologies and biotechnology, for instance, are all indicative of the utopian and dystopian accounts that tend to accompany new or refashioned developments. The current reach and magnitude of big data, however, do warrant some critical attention in ways that entertain a more nuanced and less deterministic view, and especially in light of the increasing deployment of big data in the management of borders and immigration.

For the purpose of the present enquiry, big data are considered here primarily as an ensemble of techniques, a 'knowledge infrastructure' (Bollier, 2010: 1) involving the aggregation, computation and analysis of complex and large size contents which attempt to establish patterns and connections that can inform the process of deciding on border access, visa granting and other immigration and asylum related issues. As discussed below, this knowledge infrastructure is rather intricate and multi-layered and demonstrates the increasing interest in and reliance on data-driven strategies to manage border and migration.

Augmented borders

In a sense, the incorporation of big data into border management strategies is not only a matter of technology and data alone, but something that is indicative of the changing conceptions of borders and the practice of 'bordering' itself. As Balibar (2002) lucidly argued, borders are no longer merely static territorial dividers that concern the physical alone and separate the spatiality of one country from another. Rather, borders

have become ubiquitous, infinitely and invisibly embedded within mundane administrative processes and bureaucratic organisation. Borders are *everywhere*, or at least, 'wherever selective controls are to be found' (Balibar, 2002: 34). This can range from some ostensible practices such as stop-checks 'inside' the territory or at its shifting periphery, to some more subtle mechanisms such as access to public health services and social benefits, applying for National Insurance Number and bank accounts, and any other activity that requires a proof of *identity* as a prerequisite for access to spaces and services. These activities function as an *inner border* and a filter of legitimacy. At the same time, recent years have witnessed an increase in 'outsourced' control strategies that act as an *outer border* in that they allow control over the flux of movement across borders to be conducted at a distance. E-borders schemes and stringent visa systems in consulates located in the third countries are some of the mechanisms that seek to keep the poorest foreigners and potential asylum-seekers away as far as possible from the frontiers of developed countries (Bigo, 2005a: 6; Yuval-Davis *et al.*, 2005: 518). Broeders (2007: 72) argues that '[b]order control is "moving away from the border and outside the state" (Lahav and Guiraudon, 2000), or is becoming "remote control" (Zolberg, 2002) or is moving "upwards, downwards and outwards" (Guiraudon, 2001)'. As this extract from a report by the Australian immigration department indicates: 'Australia manages the movement of non-citizens across its border by, in effect, pushing the border offshore. This means that checking and screening starts well before a person reaches our physical border' (in Wilson and Weber, 2008: 129).

This spatial transformation of borders has been going hand in hand with developments in surveillance systems. Since 2003, Australia has been managing its 'offshore border' through Advance Passenger Processing (APP), a computerised network system, which enables 'information exchange, passenger monitoring and administrative processing to commence from the time an intending passenger applies for a visa or attempts to board a flight for Australia' (Wilson and Weber, 2008: 129). Under the APP arrangement, airlines are required to provide information on all passengers and crew, including transit travellers. This information is collected at check-in and transmitted to Australian border agencies for processing and issuing passenger boarding directives to airlines prior to the arrival of the aircraft. A chief purpose of this system is the improvement of 'risk management' techniques through data collection and processing. However, and as Bollier (2010: 14) argues, 'more data

collection doesn't mean more knowledge. It actually means much more confusion, false positives and so on.' As such efforts continue to be invested in finding and enhancing ways of managing the perceived risks associated with borders and travelling. Big data and their analytical tools are some of the recent technologies that are being fast-tracked to enable more sophisticated ways of tracking the movement of perceived 'risky' passengers.

In 2013, the Australian Customs and Border Protection Service (ACBPS) implemented an advanced passenger solution that uses big data analytics developed by IBM to improve border security. The solution is designed to eliminate the need of manually pulling data from multiple systems by automating the process of data collection and analysis. Customs' officials can now collect and store Passenger Name Record (PNR) data from travel agents, airline companies and other entities, and receive real-time information about all departures and arrivals (Karlovsky, 2013; Sweeney, 2013). The collected records, which comprise of an extensive set of approximately 106 different data fields (Braue, 2013) are then processed and 'risk-assessed' to build profiles of so-called high risk passengers and ensure greater precision in securing Australia's borders. It is expected that such use of PNR data would expand to 29 countries as big data solutions like ACBPS-IBM system are increasingly rolled out (Braue, 2013). In early 2011, a prototype of this system was deployed in Melbourne, Sydney and Brisbane airports. According to the Australian government,

> the system had halved the number of travellers undergoing additional checks at airport immigration points whilst detecting an increased number of suspicious travellers, many of which were eventually refused entry to Australia. The effectiveness of the system in turn saved tax payer dollars at an average of $60,000 saved per refusal. In using advanced analytics, DIAC has substantially enhanced its ability to accurately identify risk while also reducing the need for delaying incoming travellers. The analytics-based system complements existing border risk identification and mitigation tools such as immigration intelligence, primary line referrals and Movement Alert List matches. (*Big data Strategy*, 2013)

In a rather unusually revealing presentation, Klaus Felsche (2012), Director of Intent Management & Analytics at the Australian Department of Immigration and Citizenship, explains in some detail the process of data capture, storage and analysis pertaining to the layered approach to border management in Australia:

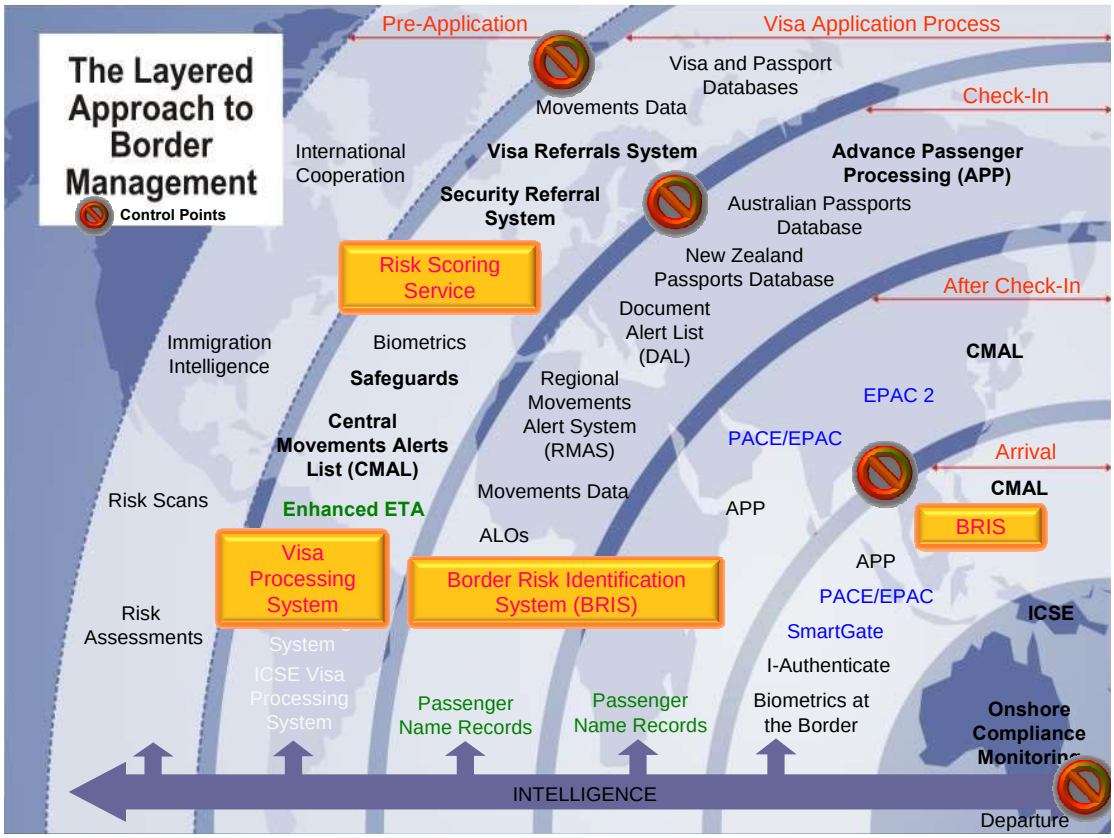

Figure 1: Felsche, 2012

As can be seen through the above illustration, database systems and advanced analytical procedures, such as the BRIS system, underline and inform much of the life cycle of border management processes. From pre-application all the way to arrival, travellers are increasingly being subjected to sophisticated and automated systems of profiling and risk analysis. Felsche argues that whereas in the past customs relied mainly on instinct in reading body language and screening passengers, and on time-consuming mass interviews, now with the new big data analytics of the BRIS system, border officers are able to predict 'risky travellers', catch and deport more people conducting less interviews and using fewer resources: 'The computer can't see whether someone in the arrivals hall is sweating but it sure as hell can predict that somebody should be. This means we've increased the refusal rate and reduced massively the inconvenience rate for people at the airports.' (Felsche in Ramli, 2013)

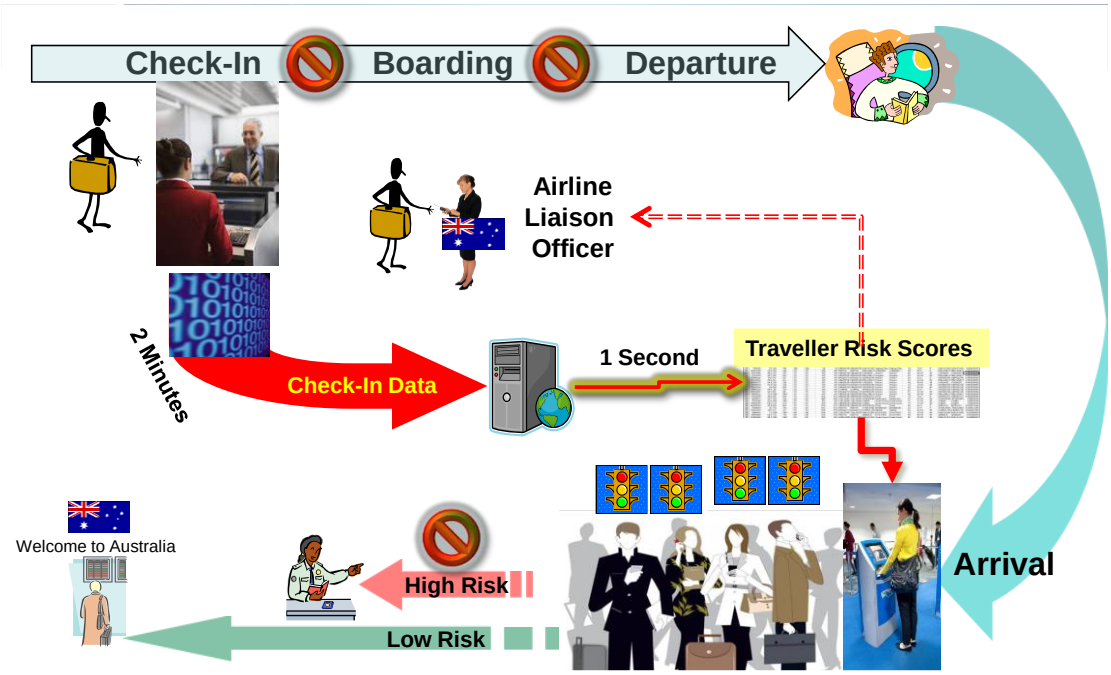

Figure 2: Felsche, n.d

As mentioned above, the system works by scanning and analysing massive amounts of data accumulated by border authorities over the years. Acting as a digital barrier for policing border movement and a tool for structuring intelligence, the BRIS system processes pre-arrival information in an 'analytical workflow' consisting of information exchange, risk scoring and passenger monitoring from the time an intending traveller purchases an air ticket to Australia or applies for a visa. This with the aim to identify in advance suspected 'high risk' passengers and facilitate the crossing of low risk ones. As stated in DIAC's annual report 2010-11, 'once identifies, [high risk] passengers are referred to airport liaison officers (ALO) and border officers for intervention […] When combined with random inspections, pre-arrival data can significantly augment threat identification and interdiction, thus improving an administration's effectiveness in meeting national economic and security mandates.' (DIAC, 2011)

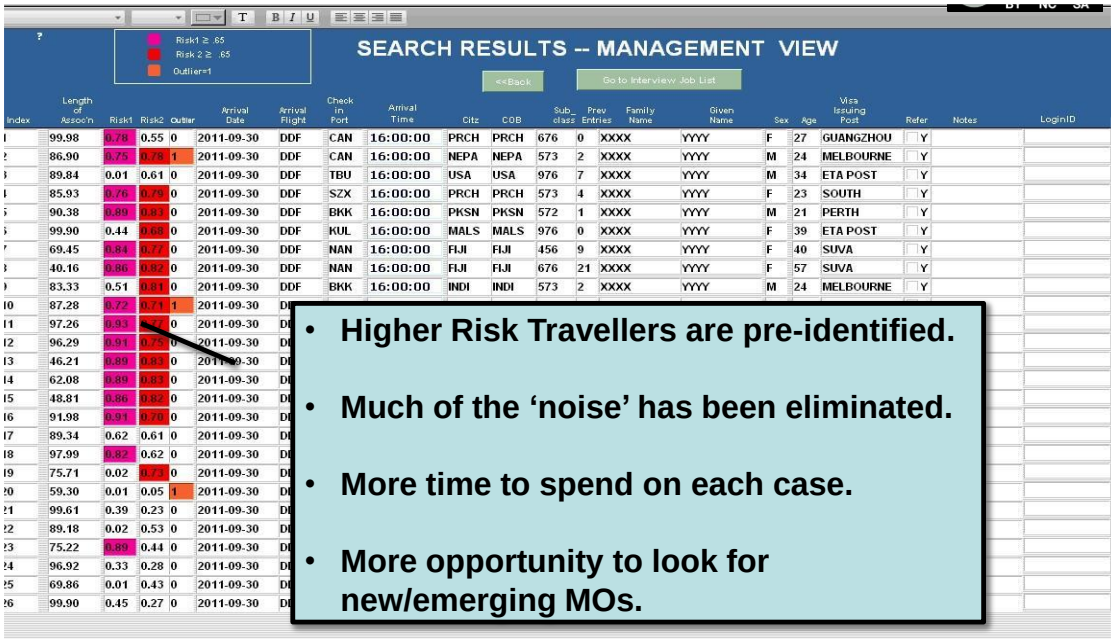

Figure 3: Felsche, n.d

Underlying these preemptive data analytics-driven developments in the field of border control is the belief that 'Customs Organizations are generally "Data Rich", but "Knowledge Poor"' (Thibedeau, 2013) and, as such, in need of advanced data mining techniques and analytical solutions to fine tune the knowledge produced out of data processing and to structure in better ways the resulting intelligence. The argument is that automated surveillance systems, such as BRIS, make border control far more rigorous than what was previously possible. Under automated control, it is argued that border authorities have a more extended ability to detect and deter clandestine entries compared to control under manual patrol. This statement is a case in point: '[a]dopting an automated risk assessment system is a significant step towards successfully adopting risk management practices strategically, operationally, and tactically. Border control processes that use risk assessment systems help ensure that customs resources are always focused on the highest risk shipments and people in real time' (Thibedeau, 2013). However such automated systems and risk management techniques raise a number of ethical concerns that can hardly be avoided. In what follows, I reflect on some of these issues.

Categorisation

At the heart of these predictive mechanisms of control is a process of sorting and categorisation which undoubtedly poses one of the pertinent ethical issues vis-à-vis the politics of borders and their securitisation through big data tools. For such techniques enable the systematic ordering and classification of the moving population

body into pattern types and distinct categories, a process that contribute to labelling some people as risky and others as legitimate travellers, and demarcating the boundaries between them. Borders are indeed, as Balibar (2002: 81, 82) argues, designed to establish 'an international class differentiation', 'a world apartheid', 'a dual regime for the circulation of individuals'. They are highly 'polysemic' and 'heterogeneous' zones (ibid.), the crossing of which does not necessarily create the same phenomenological experience for everyone. While some passengers are endowed with the right to smooth passage and reduced delay, others are made to endure an 'excess of bordering', sometimes before even leaving the country of origin and embarking on their journeys, all being based on the projections and predictions of integrated risk management tools. As Amoore (2006: 340) argues, '[the] risk-based identity of the person who attempts to cross an international border is in this way encoded and fixed far in advance of reaching the physical border - when, for example, he leaves the electronic traces of buying an air ticket, applying for a visa, using a credit card, and so on.' The use of risk management techniques enables various profiling mechanisms and deductive classifications to systematically sort among people and formulate what and who must be monitored (Bigo, 2006a: 39). In supporting the use of big data in borders and in the security field, Alan Bersin, from the U.S. Department of Homeland Security, describes the profiling process in the following terms: '"high-risk" items and people are as "needles in haystacks". [Instead] of checking each piece of straw, [one] needs to "make the haystack smaller," by separating low-risk traffic from high-risk goods or people.' (in Goldberg, 2013).

In this movement between macroscopic and microscopic perspectives on risk through big data analytics, there is the danger of augmenting the function of borders as spaces of 'triage' whereby some identities are given the privilege of quick passage whereas other identities are arrested (literally). With big data comes 'big borders' through which the scope of control and monopoly over the freedom of movement can be intensified in ways that are bound to reinforce further 'the advantages of some and the disadvantages of others' (Bigo, 2006b: 57) and contribute to the enduring inequality underpinning international circulation and its multiplying forms of exclusion. The management of borders through technology is indeed very much about creating the means by which freedom of mobility can be enabled, smoothened and facilitated for the qualified elite; the belonging citizens, all the while allowing the allocation of more time and effort for additional security checks to be exercised on those who are

considered as ‘high risk’ categories. Governments and companies often promote the illusion that algorithmic processes and data-driven systems are purged from human bias and interference leading to more neutral, objective and automated decisions that are devoid of instances of discrimination on the basis of race, ethnicity, etc. (Muller, 2004; Dworkd and Mulligan, 2013). For instance, and in reference to the BRIS system, Felsche (in Wheatley, 2013) argues that ‘The beauty with this analytics process is we are on solid ground because it’s all in the data, and I know the system works when we ping the first Brit or the first American or the first Swede because that means it is agnostic.’ However, the reality is far from being the case and is rather a messier ‘mix of technical and human curating’ (Dworkd and Mulligan, 2013) which inevitably involves bias and prejudice:

> Both the datasets and the algorithms reflect choices, among others, about data, connections, inferences, interpretation, and thresholds for inclusion that advance a specific purpose […] classification systems are neither neutral nor objective, but are biased toward their purposes. They reflect the explicit and implicit values of their designers. Few designers “see them as artifacts embodying moral and aesthetic choices” or recognize the powerful role they play in crafting “people’s identities, aspirations, and dignity” […] The urge to classify is human. The lever of big data, however, brings ubiquitous classification, demanding greater attention to the values embedded and reflected in classifications, and the roles they play in shaping public and private life. (ibid.)

In terms of immigration, the risk is that, through big data, governments can target and ‘track undocumented migrants with an unheard of ease, prevent refugee flows from entering their countries, and track remittances and travel in ways that put migrants at new risks.’(Lee, 2013). The use of big data can thus become an immobilising act of force that suppresses the movement of certain categories and restricts their access to spaces and services. For instance, a simple search on Google for popular immigration-related topics like “moving to Australia” or “EU asylum law” can indicate intent to move or migrate (ibid.). Data collected trough search engines can be saved and later on analysed opening up the potential for profiling and surveillance. With big data, the possibilities of control might be endless: governments might be able to

> predict the next refugee wave by tracking purchases, money transfers and search terms prior to the last major wave. Or connect the locations of recipients of text messages and emails to construct an international network and identify people vulnerable to making the big move to join their family or spouse abroad. (If the NSA can do it, why not Frontex?) Or, an even more sinister possibility- identify undocumented migrant clusters with greater accuracy than ever before by comparing identity and location data with government statistics on who is legally registered. (ibid.)

Often couched in terms of efficiency, value for tax payers and utilitarian convenience, the use of big data for border management acquires its legitimacy by constructing a divide between the 'belonging citizens' and 'risky others', attaching itself to things that are valued by the public, such as security and the welfare system, and staging a need for their protection and securitisation. This in turn ends up perpetuating the dividing discourses and conceptions of "us and them", the "ins and outs", that have become prevalent features in immigration and borders management policies, reinforcing forms of marginalisation and prejudice that are often associated with processes of 'othering' and casting certain groups as a 'threat' (see van Dijk, 1995). As it stands at the moment, many of the existing debates on the issue of privacy and data protection legislations with regard to big data and its related techniques tend to narrowly focus on the category of the 'citizen' as their primary subject, leaving behind many vulnerable groups, such as asylum seekers and undocumented migrants, who are often, as a result of the legal system itself, excluded from such a category.

In fact, big data techniques and their categorising mechanisms raise the very foundational question of what it means to be 'human' nowadays. Far from being this presumably 'universalistic' and all-inclusive category, humanity has for so long 'operated through systematic technologies of inclusion/exclusion' (Bhandar, 2004: 271) that are informed by a defective thinking of what constitutes the human in the first place. Judith Butler (2003) argues that oftentimes it is the dominant assumptions about the human and its conflation with artificial categories such as the 'citizen' that threaten to leave those who are perceived as 'others' in a no-man's land whereby their humanity is in danger of being left unrecognised and unacknowledged. This is evident in the ways in which asylum seekers and immigrants are often treated and regarded. From the 'boat-people operation' in Australia whereby military force is being used to

deter asylum seekers from entering the Australian shores[2] to the recent tragic events in Lampedusa and the subsequent degrading mistreatments of migrants at the reception centre of the island[3], what is at stake is precisely the status of the human whose crisis is currently striking at the heart of not only so-called undemocratic, undeveloped or failed states but also right at the very centre of modern democracies and their much-vaunted 'human rights' systems. Who is this 'human' in human rights? And whose rights these systems are laying claim to?

Faced with the plight of the millions of refugees and the displaced every day, these systems, originally founded on the declarations of 1789 and 1948, are now left trembling in the face of a reality in which, as Hannah Arendt (1966) once argued, being forced out of the nation-state often threatens to become tantamount to the expulsion from humanity itself. Arendt and later on Agamben have repeatedly pointed out that the very origin of human rights is based on the assumption that the human *is* the citizen, an assumption that turned up to be the source of much tension, contention and even violence, both politically and ontologically. In the system of the nation-state, Agamben (2008: 92) writes, 'so-called sacred human rights are revealed to be without any protection precisely when it is no longer possible to conceive of them as rights of the citizens of a state […] That there is no autonomous space in the political order of the nation-state for something like the "pure human" is evident at the very least from the fact that the status of refugee has always been considered a temporary condition that ought to lead either to naturalization or to repatriation. A stable statute for the human in itself is inconceivable in the law of the nation-state'. If that is the case, what becomes, then, of those who are no longer citizens or political subjects? Those who have lost every quality except for the pure fact of being human *tout court*? This is precisely the predicament that continues to face many refugees and undocumented migrants, and also the question that constitutes a crisis at the heart of the logic of the nation-state and its founding categories. For once the flimsy support of citizenship is taken away, what is left exposed is precisely that nakedness and fragility of the human *qua* human, a status that cries out for a redefinition of the human beyond the ascriptions of citizenship, politics and identity itself, so that this notion of the human becomes more inclusive, more extensive, more indiscriminatory and hopefully more 'human'. The stakes are indeed, as Jacques Ranciere (2004)[4] argues, a matter of redefining the human as the radical dismissal of any difference between those who are citizens and those who are not, those who are qualified to participate in politics and

those who are not. Humanity for all where no one is illegal.

Politics of borders, however, seem to be heading in the opposite direction. At a time when the number of refugees is on the rise, governments across the world are praising themselves on the reduction in asylum applications and continue to invest in mechanisms that only exacerbate xenophobia and intolerance. The deployment of big data techniques in the management of borders at a distance is indeed yet another development in which the othering and control of certain people is in danger of becoming a routine and normalised practice if left unchallenged and unscrutinised.

Projection

Much of big data analytics and the risk management culture within which it is embedded are based on acts of 'projection' that are often mediated through an emotional landscape of fear, distrust and suspicion. Fear indeed is becoming a powerful tool of governing and regulating populations (van Munster, 2005: 22) and a driving force behind the governmental desire to master the future so as to predict and preempt certain events and actions. 'This monitoring or management of the uncertainty of tomorrow is associated with technologies of profiling, data mining, and constitutions of risk group categories whose main goal is to assess the future through the knowledge of patterns derived from the past in order to act on time, to have a grip on the present' (Bigo and Delmas-Marty, 2011). The future, as such, is increasingly becoming the object of calculative technologies of simulation and speculative algorithmic probabilities, resulting in what Bigo (2006a: 58) refers to as 'the fictionalisation of the world', a simulacrum of sorts whereby paranoid scenarios loom large. The ramification of such an approach towards the future has often been the paradoxical increase in instances of endangerment and insecurity rather than their total preemption. Recursively, what follows is the mobilisation of more preemptive techniques and security technologies, and the construction of various images of otherness and dangerousness, all being based upon the enduring belief that one can create 'a grammar of futur antérieur' by which the future can be read as a form of the past in order to manage risk and prevent unwanted events (ibid.: 61). Big data promise to offer such grammar through their visualisation techniques and predictive algorithms, through their correlations and causations. As Kerr and Earle (2013) explain, through 'the formulaic use of zetabytes of data to anticipate everything from consumer preferences and customer creditworthiness to fraud detection, health risks,

and crime prevention […,] big data promises opportunities like never before to anticipate future needs and concerns, plan strategically, avoid loss, and manage risk.'

Despite these promises, however, big data analytics raises concern vis-à-vis its power to enable 'a dangerous new philosophy of preemption' (ibid.), one that operates by unduly making assumptions and forming views about others without even 'encountering' them. By gathering information and constructing profiles of individuals and groups, governments and companies are increasingly reliant on algorithms to anticipate certain actions and predict their likely consequences with the view to eschew risk and forestall unwanted actions. Preemptive predictions and their resulting future-oriented projections are 'intentionally used to diminish a person's range of future options', to allow or disallow a person to act in a certain way (ibid.). In the context of big data's use in border management and immigration control, this translates into acts of power, performed from the standpoint of governments and corporations, which result into the construction of 'no-fly lists', the identification of potentially risky individuals, and the prevention of activities that are perceived to generate risk, including the movement of potential asylum seekers and refugees. According to Kerr and Earle (2013), such preemption strategies come at a significant cost:

> As an illustration, consider the practice of using predictive algorithms to generate no-fly lists. Before the development of many such lists in various countries, high-risk individuals were generally at liberty to travel—unless the government had a sufficient reason to believe that such individuals were in the process of committing an offense. In addition to curtailing liberty, a no-fly list that employs predictive algorithms preempts the need for any evidence or constitutional safeguards. Prediction simply replaces the need for proof. [A] universalised preemption strategy could challenge some of our most fundamental jurisprudential commitments, including the presumption of innocence […] Taken to its logical extreme, the preemption philosophy is not merely proactive—it is aggressive. (ibid.)

What is at issue in this preemption philosophy is also a sense of reduced individual agency. The subjects of big data predictions are often unaware of the content and the scale of information generated about them. They are often unable to respond to or contest the 'categorical assumptions' made about their behaviours and activities, and

the ensuing projections that affect many aspects of their lives, rights and entitlements. They are left without the chance to challenge the measures and policies that affect them in fundamental ways, such as criteria of access and so on. What happens then to those who appear as hits on the various digital archives and databases? Or more importantly, 'how a "false hit" that leads to detention or deportation can be challenged [?] As one EPIC lawyer put the problem: "these technologies are assumed to provide a complete picture of who someone is, leaving people having to dispute their own identity"' (Amoore, 2006: 340).

The power of the panoptic gaze that is afforded by big data techniques is certainly one of imbalance to the extent that it allows governmental and private entities to expand and deepen their field of view, and make decisions that implicate people without them even knowing about it. Given the lack of transparency and the one-way character of big data surveillance, people are kept unaware of the nature and extent of such surveillance and are thus prevented from controlling aspects of their data and responding to surveillance activities. For without the needed procedural transparency and access to adequate information, individuals remain in the dark with regard to what kind of data are being collected about them, how these data are being processed and for what purpose. Autonomy and the ability to act in an informed and meaningful way are significantly impaired, as a result. We are, as such, at risk of 'being defined by algorithms we can't control'[5] as the management of life and the living becomes increasingly reliant on data and feedback loops. In this respect, one of the ethical challenges is certainly a matter of 'setting boundaries around the kinds of institutional assumptions that can and cannot be made about people, particularly when important life chances and opportunities hang in the balance' (Kerr and Earle, 2013). Circulation and movement are no exception.

Another important ethical challenge concerns the treatment of the 'future itself'. Increasingly, and as Bigo and Delmas-Marty (2011) rightly argues, the 'colonisation' of the future is becoming a major feature in the governance of various fields and spaces including those of borders and transnational mobility. The preemptive discourse that has been underlying many governance strategies, including those of immigration and asylum, is now taking a step further: it is no longer enough to

> assess possible futures, to do simulation and alternative scenarios and to guess what virtual future has the most chance to become actualised, now the

> professionals of security technologies want to reduce all these possible futures to only one future; often the future of the worst case scenario. And it is this selected future that they read as a future perfect, as a future already fixed, a future they already know. [This] is the by-product of the existence of transnational guilds of professionals of (in)security who share the same view of the world to come. (Bigo and Delmas-Marty, 2011)

A dangerous step, no doubt, given how this modality of governing through fear and insecurity ends up closing off the horizon of futurity and cancelling out its potentialities. Seeing the world through the distorted filters of fear has been fuelling many illiberal practices and justifying the adoption of various exceptionalist methods of intervention and preemption (see Agamben, 1998; Bigo, 2005a, 2005b; Muller, 2004). While the preemptive attitudes towards the future are operating in the name of security, safety, and the fight against terrorism and other social ills, they are also lacking a sense of awareness that 'the present situation is also the fault of the will to master the world, to try to control some part of it by 'scientifically' discriminating the enemy within, and to believe that technology can do it' (Bigo, 2006b: 62) – all too often, technology merely functions as an 'improved means for unimproved ends' (Webster, 2000: 86). These attitudes are also a manifestation of a parochial style of thinking and governing. By favoring a technocratic approach as opposed to questioning the very power structures and dynamics that are at the base of the world's staggering inequalities, oppressions and socio-political troubles (which often lead to forced migration), these fear-driven governmental attitudes end up tearing issues of borders, immigration and asylum away from their historical and political context, and separating them from 'human rights and social justice frameworks' (Wilson and Weber, 2008: 135). One should not ignore the fact that the enduring legacies of colonialism together with a rising neoliberal globalisation are all some of the undeniable factors that have been increasing the wealth of some nations while impoverishing others (see Pogge, 2008) and leading to the uneven distribution of the freedom of movement. Staging the issues of immigration and borders as if they were stand-alone decontextualised security problems is rather irresponsible and misses the bigger picture.

(Dis)embodied Identity

The issues discussed above inevitably lead us to the question of identity, which remains at the heart of the manifold concerns surrounding big data tools and techniques. In risk management and profiling mechanisms, identity is 'assumed to be anchored as a source of prediction and prevention' (Amoore, 2006: 336) to the extent that 'identity crime', for instance, is seen as a key element in many of the threats (real or imagined) believed to be facing contemporary societies. As this statement by the former UK Prime Minister Tony Blair indicates, '[o]n any list of public concerns, illegal immigration, crime, terrorism and identity fraud would figure towards the top. In each, identity abuse is a crucial component.' (Blair, 2006). Such argument stems from the belief that those in breach of immigration law, those engaging in illegal work or unauthorised employment, those committing acts of crime and terrorism, etc., all rely in one way or another on the relative ease by which one can build a new and false identity, appropriate someone else's identity, or gain unauthorised access to personal data and financial information. For instance, '[t]errorists routinely use multiple identities – up to 50 at a time – to hide and confuse. This is something al-Qa'eda train people at their camps to do' (ibid.). Identity-related crimes are thus framed as a specific kind of fluid risk that pervades a myriad of spaces and activities and whose management requires various securitisation strategies and techniques (Ajana, 2013). At the same time, identity is also seen as a valuable 'asset' that enables the actualisation of one's autonomy and freedom of choice within the circuits of consumption: '[y]our identity is a valuable commodity – you need it to function in everyday life' (CIFAS, 2007). With regard to immigration and borders management, identity is indeed one of the primary targets of security technologies whether in terms of the use of biometrics to *fix* identity to the person's 'body' for the purpose of identification and identity authentication (Ajana, 2013) or in terms of the deployment of big data analytics to construct predictive profiles to establish who might be a 'risky' traveller, as discussed earlier.

In this normative thinking of identity as either an asset or a traceable trail for security forensics, one can identify a dual process taking place: a 'de-combining' and 'recombining' of identity-as-data and the embodied subject. That is to say, on the one hand, the proliferation of data and profiles across networks and platforms gives the impression that identity is increasingly 'abstracted' from the so-called physical self in a way that indicates a somewhat Cartesian approach to body and mind in big data science. On the other hand, data collected on individuals remain embodied through and through not least in terms of the way in which digital profiles and the information generated

about individuals and groups end up affecting their very material existence, embodied experiences, and life chances (from physically being able to cross borders to accessing social services, healthcare and so on). As van der Ploeg (2003: 58) argues, 'the translation of (aspects of) our physical existence into digital code and "information", and the new uses of bodies this subsequently allows, amounts to a change on the level of ontology, instead of merely that of representation".

Big data techniques approach, and sometimes reduce, individuals to what Deleuze (1992) calls 'dividuals'; bits and digits dispersed across a multitude of databases and networks, and identified by their profiles, pins, tokens, credit scoring, etc. rather than their subjectivities. They do not address people as ''whole persons' with a coherent, situated self and a biography, but rather make decisions on the bases of singular signs' (Aas, 2006: 155). At the same time, this dividuation through big data also facilitates the 'reassembling' of those bits and signs into digital profiles whereby identities are put together or constructed from scratch in ways that imbue those profiles with a life of their own (a life that might even negate, wipe out, or at least, momentarily override the 'lived life' of the person under scrutiny, as it is often the case with asylum seekers). And through this process, individuality can (re)emerge again, producing what Ajana (2010: 248) terms a 'recombinant identity'. This is a quasi-artificial, but by no means disembodied, identity generated through the combining of various data and whose institutionalisation and manifestation often interfere with and affect the life course of the person. It is an identity that is certainly marked by 'a power relation' insofar as the knowledge it emerges from is one that is based not on 'mutual communication', but on 'one-way observation' (Aas, 206: 153); on official sources and technical operations that diminish 'the space for individual explanation and narrative, with the result that individuals are no longer part of their own identity-making' (Rygiel, 2010: 146).

In a sense, the recombinants identities that are produced through big data resemble Haggerty's and Ericson's (2000) notion of 'data doubles', a concept they use to refer to the process of breaking down and abstracting the individual subject into a series of data. However, while these 'data doubles' mainly designate a 'decorporealised body' and an 'abstract' type of individuality that is comprised of 'pure virtuality' and 'pure information' (Haggerty and Ericson, 2000: 611-614), the recombinant identities generated by big data, on the other hand, indicates the 'actuality' of re-individuation, that is to say, the terminal point at which data recombine into an identity in the 'concrete',

'corporeal' and 'material' sense. In this context, never, at any stage, could data be considered as 'purely' virtual, decorporealised, disembodied or immaterial (Ajana, 2010: 248).

Relating this to our discussion on borders, one can imagine how one's data double travels 'in advance' to the point of arrival through the various information networks and circuits, and waits for the physical referent (the body) to arrive. At arrival, and sometimes even before, the data double is matched with the body as well as with other categorical data associated with behavioural patterns and levels of dangerousness, and recombine into an actual identity that is, accordingly, either granted or denied access. As Bigo and Delmas-Marty (2011) explain, 'like your guardian angel, your data double travels first through the flow of information coming from diverse interconnected databases. If clean enough, then you will travel safely, if not you will have trouble […] and the tendency of this data double to have an autonomous life increases with each travel across databases'. As such, this ontological and temporal décalage between data and actual self need not be considered as a disembodied process but one that incessantly and dialectically oscillates between the physical and the informational, between the virtual and the actual.

Emphasising this recombining and embodied aspect of big data is important as it challenges the dominant conceptualisations of identity in big data science whereby individuals are rarely regarded in terms of their anthropological embeddedness and embodied nature, the result of which is often a loss of ethical and socio-political considerations as well as the increasing commodification of identity. More crucially, this emphasis on the embodied dimension helps bringing awareness of the paradoxical fact that big data tools and analytics produce profiles and identities that are at once *independent* of the story of the person, and yet 'undeniably belonging to that person' (van der Ploeg, 1999: 300). '[y]ou cannot control the matching of your data with other data. It goes beyond the traditional notion of privacy. It has to do with a statistical approach to surveillance, which prohibits the movement of the most suspicious […] of the travelling population in order for the others to be at ease' (Bigo and Delmas-Marty, 2011). This in turn poses many ethical challenges in terms of the ways in which practices of big data surveillance and identification end up partaking of processes that *impose* certain identities while obstructing others, endorse certain identities while criminalising

others, thereby affecting the embodied existence of the person. As Bauman (2004: 13) rightly argues:

> 'Identities' float in the air, some of one's own choice but others inflated and launched by those around, and one needs to be constantly on the alert to defend the first against the second; there is a heightened likelihood of misunderstanding, and the outcome of the negotiation forever hangs in the balance.

This is particularly true of marginalised groups, such as immigrants and asylum seekers, whose lives and biographies are continuously being caught up in domains of power and shaped by their Sisyphean interactions with bureaucratic institutions and the forms of identities that are often imposed upon them as a result of such interactions. An embodied approach to big data and identity is, therefore, necessary to move the ethical debate forward and contest the ever-increasing abstraction of people and the resulting material ramifications. This requires the rethinking of the entire normative framework through which the relationship between identity, data and body is understood and conceptualised, and challenging the taken for granted distinction between 'embodied identity or physical existence […] and information about (embodied) persons' (van der Ploeg, 2003: 58). For, identity cannot be dissociated from the embodied experience nor can it be extracted merely from the collection of data and information. When identity is viewed through the lens of embodiment, what ensues is a problematisation of the very distinction between materiality and immateriality and, with it, the distinction between the 'material' body/identity and body/identity as data, a distinction that often goes unquestioned within the big data industry and its capitalist ideology. Attending to the ways in which the use of big data 'translates in the *lives* of people' (van der Ploeg, 2005: 13, my italics) is doubtless an important and urgent ethical task.

Conclusion

The adoption of big data analytics in the fields of border management and immigration control signals yet another step towards the intensification and automation of preemptive ICT-based surveillance. In this paper, I drew on the example of Australia's ACBPS-IBM system as an entry point to discussing some of

the ethical issues pertaining to the collection, use and manipulation of large data sets relating to travellers. I argued that the use of such big data systems risks *augmenting* the function and intensity of borders, raising many ethical and political questions. Our discussion revolved around three key points. First, I highlighted the issue of categorisation as being at the base of border management practices. The deployment of big data tools can enable more refined and sophisticated classification processes whose purpose is to demarcate between so-called 'legitimate travellers' and 'risky passengers'. Such categorisations often lead to reinforcing forms of inequality and discrimination and modes of oppression that have become hallmarks of recent immigration policies. The second point concerns the danger of projection that inheres within the predictive and future-oriented nature of big data analytics. Through their preemption philosophy, big data tools enable the systematic profiling of people and the forming of assumptions about their character, behaviour, activities and risk potential without even encountering them. This, I argued, raises many ethical issues not least in terms of the prejudice such profiles can create, the imbalanced nature of the knowledge and power dynamics produced through big data analytics, and the incessant foreclosure of the future as a result of too much control and prediction. Lastly, I addressed the question of identity and its relation to big data, with a particular focus on the issue of embodiment. Very often, big data, or data in general, are seen as that which is immaterial and disembodied, as separate from the physical subject. The danger of such perception, I argued, is the precluding of social and ethical considerations when addressing the implications of big data on identity as well as the reduction of the latter into an asset, a commodity. I therefore emphasised the importance of an embodied approach to contest this presumed separation between data and their physical referent. This is crucial, especially when the identities at issue are those of vulnerable groups such as asylum seekers and refugees.

Although the focus of this paper has been mainly on the negative implications of using big data in the field of borders and immigration management, it is worth pointing out that big data can also hold the potential to benefit vulnerable groups if deployed with an ethics of care and in the spirit of helping migrants and refugees as opposed to controlling them. For instance, one benefit relates to the ways in which big data can enable migration scholars and activists to overcome the lack of accurate statistics that continue to plague the field of migration studies and research (Lee, 2013). This lack of quantitative data has for so long been exploited by sensationalist

media outlets and right wing politicians who, through distorted statistics and attendant discourses, perpetuate anti-immigration sentiments and exaggerate the supposed 'influx' of migrants and asylum seekers. In addition and as Hermanin (in ibid.) argues, '"no data available" is a common excuse for not doing more to fight discrimination and inequality'. As such, harnessing the potential of big data in providing more accurate statistics can help fighting back against 'fear-mongering false statistics in the media' and providing scholars and activists with new ways of understanding the flows of migration and enhancing humanitarian processes (Lee, 2013).

Therefore, rather than simply demonising or celebrating big data developments, I believe that the ethical impetrative lies in ensuring that theorists and ethicists of technology and data science are well ahead in comprehending the manifold meanings and implications of big data, and active in influencing minds and hearts, policies and laws, about issues concerning immigration and asylum. For without this and before we know it, big data may as well join the string of other technologies that have been deployed to criminalise rather than help those who are in need of protection and welcoming.

Notes

[1] Throughout this paper, I refer to big data in plural, as the singular of data is 'datum'.
[2] See Kathy Marks (2014), http://www.independent.co.uk/news/world/australasia/australian-government-uses-military-to-repel-boat-people-but-is-silent-on-claims-of-savage-treatment-9062559.html
[3] See BBC (2013), http://www.bbc.co.uk/news/world-europe-25510864
[4] See also Andrew Schaap (2011), 'Enacting the right to have rights: Jacques Ranciere's critique of Hannah Arendt'.
[5] See Lowe and Steenson (2013), http://schedule.sxsw.com/2013/events/event_IAP5064

References

Aas, K.F. (2006) ''The body does not lie': Identity, risk and trust in technoculture', *Crime Media Culture*, vol.2, no. 2, 143-158.

Amoore, L. (2006) 'Biometric borders: Governing mobilities in the war on terror', *Political Geography*, vol. 25, 336-351.

Agamben, G. (1998) *Homo Sacer: Sovereign Power and Bare Life*, Stanford University Press.

Agamben, G. (2008) 'Beyond Human Rights', http://www.casadosaber.com.br/sabermais/2755/Agamben.BeyondHumanRights.pdf
Arendt, H. (1966) *The origins of totalitarianism*, London: Harcourt Brace Jovanovitch.

Ajana, B. (2013) *Governing through Biometrics: The Biopolitics of Identity*. Basingstoke: Palgrave Macmillan.

Ajana, B. (2010) 'Recombinant Identities: Biometrics and Narrative Bioethics', *Journal of Bioethical Inquiry*, vol.7, no.2, pp.237–258.

Australian Government Information Management Office (2013) 'The Australian Public Service Big Data Strategy', http://www.finance.gov.au/sites/default/files/Big%20Data%20Strategy.pdf

Balibar, E. (2002) *Politics and the other scene*. London: Verso.

Bauman, Z. (2004) *Identity*, Cambridge. UK: Polity Press.

BBC (2013) 'Italy clearing Lampedusa migrant centre', http://www.bbc.co.uk/news/world-europe-25510864

Bhandar, D. (2004) 'Renormalizing Citizenship and Life in Fortress North America', *Citizenship Studies*, vol. 8, no. 3, 261-278.

Bigo, D. (2005a) 'Globalized-in-security: the Field and the Ban-opticon', http://www.wmin.ac.uk/sshl/pdf/CSDBigo170106.pdf

Bigo, D. (2005b) 'Exception and Ban: discussing the "state of exception"', http://ciph.org/fichiers_pdfdivers/Interventions_2.pdf

Bigo, D. (2006a) 'Globalized (in)Security: the Field and the Ban-opticon', in Bigo, D. and Tsoukala, A. (eds), *Illiberal Practices of Liberal Regimes – the (in)security Games*, Paris: L'Hartmattan.

Bigo, D. (2006b) 'Security, exception, ban and surveillance', in Lyon, D. (ed), *Theorising Surveillance: The panopticon and beyond*, Devon: Willan Publishing.

Bigo, D. and Delmas-Marty, M. (2011) 'The State and Surveillance: Fear and Control', http://cle.ens-lyon.fr/anglais/the-state-and-surveillance-fear-and-control-131675.kjsp?RH=CDL_ANG100100#P4

Blair, T. (2006) 'PM defends ID cards scheme for The Daily Telegraph', http://www.pm.gov.uk/output/Page10360.asp

Bollier, D. (2010), 'The Promise and Peril of Big Data', http://www.aspeninstitute.org/sites/default/files/content/docs/pubs/The_Promise_and_Peril_of_Big_Data.pdf

Boyd, D. and Crawford, K. (2011) ‘Six Provocations for Big Data’ http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431

Braue, D. (2013) ‘Customs’ big data passenger analysis respects Australian, EU privacy controls’, http://www.cso.com.au/article/524806/customs_big_data_passenger_analysis_respects_australian_eu_privacy_controls

Broeders, D. (2007) ‘The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants, *International Sociology*, vol. 22 no.1, 71-92.

Butler, J. (2003) ‘Peace is a resistance to the terrible satisfactions of war’, http://www.believermag.com/issues/200305/?read=interview_butler

CIFAS. (2007) ‘Identity fraud’, http://www.cifas.org.uk/default.asp?edit_id=566-56

Deleuze, G. (1992) ‘Postscript on the societies of control’, http://pdflibrary.files.wordpress.com/2008/02/deleuzecontrol.pdf

DIAC (2011), ‘Risk management and fraud control measures’, http://www.immi.gov.au/about/reports/annual/2010-11/html/management-accountability/corporate-governance/risk-mgt-fraud-control-measures.htm

Dwork, C. and Mulligan, D.K. (2013) ‘It's Not Privacy, and It's Not Fair’, http://www.stanfordlawreview.org/online/privacy-and-big-data/its-not-privacy-and-its-not-fair

Field Technologies Online (2013) ‘Big Data: Datalogic Predicts Growth In Advanced Data Collection As Business Analytics Systems Drive Need For More Data And Innovation’, http://www.fieldtechnologiesonline.com/doc/big-data-datalogic-data-collection-systems-data-innovation-0001

Goldberg, H. (2013) ‘Homeland Security official gives lecture on borders and big data’, http://www.michigandaily.com/news/ford-school-homeland-security-lecture

Hacking, I. (1990) ‘The Taming of Chance’, Cambridge: Cambridge University Press.

Haggerty, K.D., and Ericson. R.V. (2000) ‘The Surveillant assemblage’, *British Journal of Sociology*, vol. 51, no. 4, 605–622.

Harpertill, C. (2013) ‘Nietzsche’s ‘active forgetfulness’ in the face of the avalanche of digital data’, http://christopherharpertill.wordpress.com/tag/ian-hacking/

Karlovsky, B. (2013) ‘Big Data deployed to protect our borders’, http://news.idg.no/cw/art.cfm?id=B1DBDC39-F852-ECBB-A519BBBF1CC9C72C);

Kerr, I. and Earle, J. (2013) ‘Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy’, http://www.stanfordlawreview.org/online/privacy-and-big-data/prediction-preemption-presumption

Felsche, K. (2012), 'Real-Time Analytics Challenges for Immigration', http://papersplease.org/wp/wp-content/uploads/2012/11/cebitbigdata2012-klausfelsche.pdf

Felsche, K. (n.d), 'Future of Business Intelligence & Analytics in Financial Services', http://fst.net.au/UserFiles/Klaus%20Felsche(3).pdf

Latour, B. (2009) 'Tarde's idea of quantification', in *The Social After Gabriel Tarde: Debates and Assessments*, ed M. Candea, London: Routledge

Lee, C. (2013), 'Big Data and Migration- What's in Store?', http://noncitizensoftheworld.blogspot.co.uk/

Lowe, J. and Steenson, M. (2013), 'The New Nature vs. Nurture: Big Data & Identity', http://schedule.sxsw.com/2013/events/event_IAP5064

IBM (2013) 'IBM Big Data Platform', http://www-01.ibm.com/software/data/bigdata/

Marks, K. (2014) 'Australian government uses military to repel 'boat people' but is silent on claims of savage treatment', http://www.independent.co.uk/news/world/australasia/australian-government-uses-military-to-repel-boat-people-but-is-silent-on-claims-of-savage-treatment-9062559.html

Manovich, L. (2011) 'Trending: The Promises and the Challenges of Big Social Data', http://www.manovich.net/DOCS/Manovich_trending_paper.pdf

McKinsey Global Institute (2011) 'Big data: The next frontier for innovation, competition, and productivity', http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation

Muller, B. (2004) '(Dis)Qualified Bodies: Securitization, Citizenship and 'Identity Management', *Citizenship Studies*, vol. 8, no. 3, 279-294.

Ramli, D. (2013) 'Big data airport screening given OK', http://www.afr.com/p/technology/big_data_airport_screening_given_lOeZC83FXTfa2T9d6GbFLJ

Ranciere, J. (2004) 'Who Is the Subject of the Rights of Man?', *The South Atlantic Quarterly*, vol.103, no. 2/3, 297-310.

Rieland, R. (2012) 'Big Data or Too Much Information?', http://www.smithsonianmag.com/innovation/big-data-or-too-much-information-82491666/

Rygiel, K. (2010) *Globalizing Citizenship*, Vancouver: UBC Press.

Pogge, T. (2008) World Poverty and Human Rights: Cosmopolitan Responsibilities and Reforms, Cambridge: Polity Press.

Schaap, A. (2011) 'Enacting the right to have rights: Jacques Ranciere's critique of Hannah Arendt', *European Journal of Political Theory*, vol. 10 no. 1, 22-45

Sweeney, S. (2013) 'Australia secures borders with Big Data tools' http://www.futuregov.asia/articles/2013/sep/02/australia-secures-borders-big-data-tools/

Thibedeau, C. (2013), 'A Systems Approach to Border Risk Management', http://www.greenlinesystems.com/2013/04/16/a-systems-approach-to-border-risk-management/

van der Ploeg, I. (1999) 'The Illegal Body: 'Eurodac' and the politics of biometric identification', *Ethics and Information Technology*, vol. 1, 295-302.

van der Ploeg, I. (2003) 'Biometrics and the body as information: Normative issues of the socio-technical coding of the body', in *Surveillance as Social Sorting*, (ed) Lyon, D. London: Routledge

van der Ploeg, I. (2005) 'The Politics of Biometric Identification: Normative aspects of automated social categorization', http://www.biteproject.org/documents/politics_of_biometric_identity%20.pdf

van Dijk, T.A. (1995) 'Discourse analysis as ideology analysis', in *Language and Peace*, (eds) Schaffner, C. and Wenden, A.L. 17-36. Amsterdam: Harwood Academic Publishers.

van Munster, R. (2005) 'The EU and the Management of Immigration Risk in the Area of Freedom, Security and Justice', University of Southern Denmark Political Science Publications, http://www.sdu.dk/~/media/Files/Om_SDU/Institutter/Statskundskab/Skriftserie/05Rens12%20pdf.ashx

Webster, F. (2000), 'Information, capitalism and uncertainty', *Information, Communication & Society*, vol. 3, no. 1, 69-90.

Wheatley, M. (2013), 'Big Brother's Big Data: Locking Down Our Borders', http://siliconangle.com/blog/2012/11/07/big-brothers-big-data-locking-down-our-borders/

Wilson, D. and Weber, L. (2008), 'Surveillance, Risk and Preemption on the Australian Border, *Surveillance and Society*, vol.5, no.2, 124-141.

Yuval-Davis, N et al. (2005) 'Secure borders and safe haven and the gendered politics of belonging: Beyond social cohesion', *Ethnic and Racial Studies*, vol. 28, no. 3, 513-535.